(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 786 745 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
30.07.1997 Bulletin 1997/31

(51) Int. Cl.^{6}: G07C 9/00, G06K 9/00

(21) Application number: 97100540.0

(22) Date of filing: 15.01.1997

(84) Designated Contracting States:
AT DE FR GB IT

(30) Priority: 26.01.1996 US 592472

(71) Applicant: HARRIS CORPORATION
Melbourne, Florida 32903 (US)

(72) Inventors:
- McCalley, Karl W.
Indian Harbour Beach, FL 32937 (US)
- Setlak, Dale R.
Melbourne, FL 32934 (US)
- Wilson, Steven D.
Chicago, IL 60614 (US)
- van Vonno, Nicolaas W.
Melbourne, FL 32934 (US)
- Hewitt, Charles L.
Melbourne, FL 32935 (US)

(74) Representative: Fleuchaus, Leo, Dipl.-Ing. et al
Melchiorstrasse 42
81479 München (DE)

(54) Enhanced security fingerprint sensor package and related methods

(57) A fingerprint sensor package includes a tamper-resistant housing, a fingerprint sensor mounted in the housing, an encryption output circuit mounted within the housing and operatively connected to the fingerprint sensor for generating an encrypted output signal related to a sensed fingerprint. The fingerprint sensor package may include a processor operatively connected between the fingerprint sensor and the encryption circuit. The package includes a reference fingerprint memory for storing reference fingerprint information. The processor has the capability to determine if a sensed fingerprint matches a stored reference fingerprint. A removing circuit is provided for removing reference fingerprint information from the reference fingerprint storage means responsive to tampering.

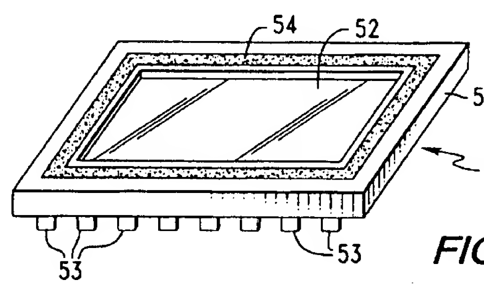


FIG. 3

CITED H #6453 WO COUNTRY
SE1334

Description

The present invention relates to the field of personal identification and verification, and, in particular, to the field of fingerprint sensing and processing.

Fingerprint sensing and matching is a reliable and widely used technique for personal identification or verification. A common approach to fingerprint identification involves scanning a sample fingerprint or an image thereof and storing the image and/or unique characteristics of the fingerprint image. The characteristics of a sample fingerprint may be compared to information for reference fingerprints already in storage to determine proper identification of a person, for verification purposes.

A typical electronic fingerprint sensor is based upon illuminating the finger surface using visible light, infrared light, or ultrasonic radiation. The reflected energy is captured with some form of camera, for example, and the resulting image is framed, digitized and stored as a static digital image, as disclosed in the specification of U.S. Patent No. 4,210,899 that discloses an optical scanning fingerprint reader cooperating with a central processing station for a secure access application. The specification of U.S. Patent No. 4,525,859 discloses a video camera for capturing a fingerprint image and uses the minutiae of the fingerprints, that is, the branches and endings of the fingerprint ridges, to determine a match with a database of reference fingerprints.

Optical sensing may be affected by stained fingers or an optical sensor may be deceived by presentation of a photograph or printed image of a fingerprint rather than a true live fingerprint.

In the event of a failure to form an acceptable image of a fingerprint, the specification of U.S. Patent No. 4,947,443 discloses a series of indicator lights which give the user a simple go or no-go indication of the acceptability of the fingerprint scanning among other potential system identification failures. In other words, another shortcoming of conventional fingerprint sensors is that inaccurate positioning of the finger relative to the sensor may reduce the ability of the processor to accurately and quickly determine a match between a sample fingerprint and a plurality of reference fingerprints.

The specification of U.S. Patent No. 4,353,056 discloses another approach to sensing a live fingerprint. In particular, it discloses an array of extremely small capacitors located in a plane parallel to the sensing surface of the device. When a finger touches the sensing surface and deforms the surface, a voltage distribution in a series connection of the capacitors may change. The voltages on each of the capacitors is determined by multiplexor techniques.

The specification of U.S. Patent No. 5,325,442 discloses a fingerprint sensor including a plurality of sensing electrodes. Active addressing of the sensing electrodes is made possible by the provision of a switching device associated with each sensing electrode.

An object of the present invention is to overcome shortcoming of conventional fingerprint sensors in that the leads and internal components of a conventional fingerprint sensor, either optical, ultrasonic or capacitive, may be tampered with, such as to send a false acceptance signal to an associated portion of equipment. Accordingly, even if the sensor is accurate and reliable, it may be readily bypassed to gain access or entry to the equipment or area intended to be protected by the fingerprint sensor.

An object of the present invention is to provide a fingerprint sensor and related methods for accurately sensing a fingerprint, and which sensor is rugged, compact, reliable and relatively inexpensive, and to provide a secure fingerprint sensing package or module and related methods for being resistant to attempts at bypassing or tampering.

Preferably, fingerprint sensor package may include a processor operatively connected between the fingerprint sensor and the encrypting output means. In addition, the package may also include reference fingerprint storage means for storing reference fingerprint information. Accordingly, the processor preferably comprises reference fingerprint matching means for determining if a sensed fingerprint matches a stored reference fingerprint. To further enhance security of the stored reference fingerprint information, the sensor package also preferably includes removing means for removing reference fingerprint information from the reference fingerprint storage means responsive to tampering.

Conveniently, the fingerprint sensor preferably comprises an integrated circuit having an outer surface portion for receiving a finger adjacent thereto. The housing, in turn, preferably includes an opening therethrough in registry with the outer surface portion of the integrated circuit. Sealing means is preferably provided for sealing an interface between the outer surface portion of the integrated circuit and adjacent housing portions. The sealing means may be provided by a bead of sealing material covering the interface. The sealing means may also be provided by a hermetic seal formed between a surrounding layer of molded plastic material and adjacent portions of the integrated circuit.

The integrated circuit may comprise an outermost silicon nitride layer for resistance to contamination, as from finger contact. In addition, the integrated circuit may have an outermost layer including one of silicon carbide and diamond for enhanced abrasion resistance.

The present invention includes a fingerprint sensor package comprising a tamper-resistant housing; a fingerprint sensor mounted in said housing; and encrypting output means mounted within said housing and operatively connected to said fingerprint sensor for generating an encrypted output signal related to a sensed fingerprint, with a processor operatively connected between said fingerprint sensor and said encrypting output means.

Advantageously, a method is for making and securely operating a fingerprint sensor package of a type including a fingerprint sensor. The method prefera-

bly comprises the steps of: mounting the fingerprint sensor within a tamper-resistant housing, and generating within the tamper-resistant housing an encrypted output signal related to a sensed fingerprint from the fingerprint sensor. The method may also include the steps of: storing reference fingerprint information within the housing, and determining within the tamper-resistant housing if a sensed fingerprint matches a stored reference fingerprint. Accordingly, for further enhancement of security, the method may also include the step of removing reference fingerprint information from within the tamper-resistant housing responsive to tampering.

The invention also includes a method for making and securely operating a fingerprint sensor package of a type including a fingerprint sensor, the method comprising the steps of:

mounting the fingerprint sensor within a tamper-resistant housing;
generating within the tamper-resistant housing an encrypted output signal related to a sensed fingerprint from the fingerprint sensor, storing reference fingerprint information within the housing and determining within the tamper-resistant housing if a sensed fingerprint matches a stored reference fingerprint.

The invention will now be described, by way of example, with references to the accompanying drawings in which;

FIG. 1 is a schematic diagram of the fingerprint sensor in combination with a notebook computer.
FIG. 2 is a schematic diagram of the fingerprint sensor in combination with a computer workstation and associated information processing computer and local area network (LAN);
FIG. 3 is a schematic perspective view of an embodiment of a fingerprint sensor;
FIG. 4 is a schematic plan view of a portion of the sensor and an overlying fingerprint pattern in with a portion thereof greatly enlarged for clarity of illustration;
FIG. 5 is a greatly enlarged plan view of a portion of the fingerprint sensor with the upper dielectric layer removed therefrom for clarity of illustration;
FIG. 6 is a schematic perspective view of a portion of the fingerprint sensor;
FIG. 7 is a schematic fragmentary view of a portion of the fingerprint sensor;
FIG. 8 is a schematic side view, partially in section, illustrating the electric fields;
FIG. 9 is a schematic circuit diagram of a portion of the fingerprint sensor;
FIG. 10 is an enlarged schematic side view, partially in section, further illustrating the electric fields;
FIG. 11 is a schematic block diagram of the fingerprint sensor and associated circuitry in one embodiment;
FIG. 12 is a schematic block diagram of the fingerprint sensor and associated circuitry in another embodiment;
FIG. 13 is a schematic block diagram of an embodiment of a sensor circuit;
FIG. 14 is a schematic block diagram of another embodiment of a sensor circuit;
FIG. 15 is a schematic block diagram illustrating a plurality of sensor units;
FIG. 16 is a schematic block diagram of an embodiment of a portion of the signal processing for the fingerprint sensor;
FIG. 17 is a schematic block diagram of another embodiment of a portion of the signal processing for the fingerprint sensor;
FIG. 18 is a schematic block diagram of yet another embodiment of signal processing circuitry for the fingerprint sensor;
FIG. 19 is a schematic circuit diagram of yet another embodiment of a portion of the signal processing for the fingerprint sensor;
FIG. 20 is a schematic circuit diagram of yet another embodiment of a portion of the signal processing for the fingerprint sensor illustrating a resistor matrix for dynamic contrast enhancement;
FIG. 21 is a schematic circuit diagram of yet another embodiment of a portion of the signal processing for the fingerprint sensor illustrating a capacitor matrix implementation for dynamic contrast enhancement;
FIG. 22 is a schematic block diagram of an embodiment of the fingerprint sensor package;
FIG. 23 is a schematic diagram of another embodiment of the fingerprint sensor package;
FIG. 24 is a schematic block diagram of another aspect of the sensor for illustrating near real-time positioning feedback of finger placement;
FIG. 25 is a schematic perspective diagram of a computer illustrating near real-time positioning feedback of finger placement; and
FIG. 26 is a schematic perspective diagram of a fingerprint sensor including indicators for illustrating near real-time positioning feedback of finger placement.

Like numbers refer to like elements throughout. The scaling of various features, particularly fingers and layers in the drawing figures, have been exaggerated for clarity of explanation.

Referring to FIGS. 1-3, the fingerprint sensor **30** is initially described. The illustrated sensor **30** includes a housing or package **51**, a dielectric layer **52** exposed on an upper surface of the package which provides a placement surface for the finger, and a plurality of signal conductors **53**. A conductive strip or electrode **54** around the periphery of the dielectric layer **52** also provides a contact electrode for the finger as described in greater detail below. The sensor **30** may provide output signals in a range of sophistication levels depending on

the level of processing incorporated in the package.

The fingerprint sensor **30** is used for personal identification or verification purposes. For example, the sensor **30** is used to permit access to a computer workstation, such as a notebook computer **35** including a keyboard **36** and associated folding display screen **37** (FIG. 1). In other words, user access to the information and programs of the notebook computer **35** may only be granted if the desired fingerprint is first sensed.

Another application of the fingerprint sensor **30** is illustrated with particular reference to FIG. 2. The sensor **30** may be used to grant or deny access to a fixed workstation **41** for a computer information system **40**. The system may include a plurality of such workstations **41** linked by a local area network (LAN) **43**, which in turn, is linked to a fingerprint identification server **43**, and an overall central computer **44**.

Referring to FIGS. 4-10, the sensor **30** includes a plurality of individual pixels or sensing elements **30a** arranged in array pattern as shown perhaps best in FIGS. 4 and 5. The sensing elements are relatively small so as to be capable of sensing the ridges **59** and intervening valleys **60** of a typical fingerprint (FIG. 4). Live fingerprint readings as from the electric field sensor **30** may be more reliable than optical sensing, because the conduction of the skin of a finger in a pattern of ridges and valleys is extremely difficult to simulate. In contrast, an optical sensor may be deceived by a readily prepared photograph or other similar image of a fingerprint, for example.

The sensor **30** includes a substrate **65**, and one or more active semiconductive layers **66** thereon. A ground plane electrode layer **68** is above the active layer **66** and separated therefrom by an insulating layer **67**. A drive electrode layer **71** is positioned over another dielectric layer **70** and is connected to an excitation drive amplifier **74**. The excitation drive signal may be typically in the range of about 1 Khz to 1 Mhz and is coherently delivered across all of the array. Accordingly, the drive or excitation electronics are thus relatively uncomplicated and the overall cost of the sensor **30** may be reduced, while the reliability is increased.

Another insulating layer **76** is on the drive electrode layer **71**, and an illustratively circularly shaped sensing electrode **78** is on the insulating layer **76**. The sensing electrode **78** may be connected to sensing electronics **73** formed in the active layer **66** as schematically illustrated.

An angularly shaped shield electrode **80** surrounds the sensing electrode **78** in spaced relation therefrom. The sensing electrode **78** and its surrounding shield electrode **80** may have other shapes, such as hexagonal, for example, to facilitate a close packed arrangement or array of pixels or sensing elements **30a**. The shield electrode **80** is an active shield which is driven by a portion of the output of the amplifier circuit **73** to help focus the electric field energy and, moreover, to thereby reduce the need to drive adjacent electrodes. Accordingly, the sensor **30** permits all of the sensing elements to be driven by a coherent drive signal in sharp contrast to prior art sensors which required that each sensing electrode be individually driven.

FIGS. 8-10 refers to the excitation electrode **71** generates a first electric field to the sensing electrode **78** and a second electric field between the sensing electrode **78** and the surface of the finger **79**, over the distances **d1** and **d2**, respectively. In other terms, a first capacitor **83** (FIG. 9) is defined between the excitation electrode **71** and the sensing electrode **78**, and a second capacitor **85** is defined between the finger skin **79** and ground. The capacitance of the second capacitor **85** varies depending on whether the sensing electrode **78** is adjacent a ridge or valley. Accordingly, the sensor **30** can be modeled as a capacitive voltage divider. The voltage sensed by the unity gain voltage follower or amplifier **73** will change as the distance **d2** changes.

In general, the sensing elements **30a** operate at very low currents and at very high impedances. For example, the output signal from each sensing electrode **78** is desirably about 5 to 10 millivolts to reduce the effects of noise and permit further processing of the signals. The approximate diameter of each sensing element **30a**, as defined by the outer dimensions of the shield electrode **80**, may be about 0.002 to 0.005 inches in diameter. The excitation dielectric layer **76** and surface dielectric layer **54** may desirably have a thickness in the range of about 1 μm. The ground plane electrode **68** shields the active electronic devices from the excitation electrode **71**. A relatively thick dielectric layer **67** will reduce the capacitance between these two structures and thereby reduce the current needed to drive the excitation electrode. The various signal feedthrough conductors for the electrodes **78, 80** to the active electronic circuitry may be readily formed as would be understood by those skilled in the art. In addition, the illustrated signal polarities may be readily reversed.

The overall contact or sensing surface for the sensor **30** may desirably be about 0.5 by 0.5 inches -- a size which may be readily manufactured and still provide a sufficiently large surface for accurate fingerprint sensing and identification. The sensor **30** in accordance with the invention is also fairly tolerant of dead pixels or sensing elements **30a**. A typical sensor **30** includes an array of about 256 by 256 pixels or sensor elements, although other array sizes are also contemplated by the present invention. The sensor **30** may also be fabricated at one time using primarily conventional semiconductor manufacturing techniques to thereby significantly reduce the manufacturing costs.

Referring to FIG. 11, functional partitioning of an apparatus **90** including the fingerprint sensor **30** is described. The fingerprint sensor apparatus **90** may be configured to provide one or more of displacement sensing of the fingerprint, provide an image present trigger, perform analog-to-digital conversion, provide full image capture and image integrity determination, provide contrast enhancement and normalization, and provide image binarization. In the illustrated embodiment,

the sensor **30** is connected to a parallel processor and memory array **92**, and control processor **93** via the illustrated interface **91**. The parallel processor **92** may provide image quality and bad block determinations; provide edge enhancement and smoothing and thinning; generate ridge flow vectors, smooth the vectors and generate ridge flow characteristics as may be desired for fingerprint matching; identify the center of the fingerprint; generate, smooth and clean curves; and provide minutiae identification. The illustrated control processor **93** may provide minutiae registration and matching, minutiae storage, generate authorization codes, and communicate with the host via the illustrated interface **94**. The illustrated local non-volatile memory **95** may also be included in the apparatus **90**.

A variation of the apparatus **90** of FIG. 11 is illustrated by the apparatus **100** of FIG. 12. This embodiment includes a two chip version of the sensor and processing electronics. The apparatus **100** includes a sensor chip **96** and an authenticator chip **97** connected via a local memory bus interface **99**. A scan control processor **98** is also included in the illustrated embodiment of FIG. 12, while the remaining functional components are the same as in FIG. 11.

Demodulation and preliminary processing of the detected signals from the sensor **30** are further understood with reference to FIGS. 13 and 14. Both of the illustrated circuits **110, 120** desirably use an alternating current excitation. In addition, the amplitude of the voltage on the sensor is proportional to the displacement of the local ground plane, hence, the signal has to be demodulated before further use. FIG. 13 illustrates a local comparator **112** to allow the control to manage the A/D conversion process in parallel. The processor can present a sequence of a reference voltages to an entire row or column of pixels or sensor elements **30a** and monitor the transitions on the **SigO** lines. A successive approximation conversion could be implemented, first stepping large steps, and then stepping in progressively finer steps over a smaller range, as would be readily understood by those skilled in the art. The **SigO** output can be a binary bus connection while the **SigA** output is a demodulated analog signal that can be used as part of analog reference voltage generating circuit.

The circuit **120** illustrated in FIG. 14 has storage to do localized contrast enhancement for all sensor units or pixels simultaneously. The computation can use the analog comparator **112** for a decision element. The binarized output image can be shifted out of the binary shift registers provided by the illustrated latches **113**. Alternately, the output image could by read out as with conventional memory array addressing as would be readily understood by those skilled in the art. Since the circuit **120** has its own local memory, it does not need a separate set of buffers to store the pixel data.

Variations in skin conductivity and contamination may cause phase shift of the electric field signal. Accordingly, the processing electronic circuits **110, 120** of FIGS. 13 and 14 preferably include a synchronous demodulator or detector **111** so that the overall circuit has less sensitivity to any such variations in conductivity.

Interconnections of the sensor units or pixels **30a** in a portion of an array are schematically illustrated in FIG. 15. Column data transfer lines **121**, row data transfer lines **122**, and comparator reference lines **123** are shown connected to the array of sensor units **30a**. The interconnections may be desirably made in an 8-by-8 block of sensor units, although other configurations are also contemplated by the present invention.

The processor circuitry is understood with reference to FIGS. 16 and 17. The circuit **130** of FIG. 16 includes a charge coupled device (CCD) shift register **131** which, in turn, includes a plurality of individual shift registers **135**. The shift registers **131** function as a tapped delay line to facilitate image signal processing. The registers **135** feed respective A/D converters **132** operated under control of the illustrated block processor **134**. The sensing amplifier outputs are connected to the CCD analog shift registers **135**, with one shift register per row of pixels. A row of data is then shifted out of the register either to an A/D converter **132** which serves as the active conversion device. Each pixel is converted to an 8 bit digital word as it arrives at the converter. The conversion process and the A-to-D reference voltage are under control of block processors, where each block processor may control one or more rows, such as, for example, 16 rows per each processor. A limited degree of dynamic contrast compensation can be achieved using data from the previous pixel conversion to scale the reference voltage; however, significant downstream digital image processing may still be required.

The circuit **140** of FIG. 17 is similar to that of FIG. 16. In FIG. 17, a comparator **141** operates under control of the illustrated block processor **134** to provide the image output signals as would be readily understood by those skilled in the art.

Turning to FIG. 18, this circuit embodiment **150** is similar to that embodiment illustrated in FIG. 11. The circuit **150** of FIG. 18 illustratively includes a 16-by-16 array of sensor units or image cells **30b** selectively addressed and read by the illustrated row select data input multiplexor **151**, column select bus drivers **153**, and comparator reference voltage dividers **152**. Once an image has been captured from the electric field sensing electrodes and digitized, fingerprint features can be extracted from the image. FIG. 18 illustrates a high level view of a sensor connected to a bank of digital signal processors **92**. A 128 x 128 pixel array, in this instance, has been partitioned into a 16 x 16 array of image cells **30b**, wherein each image cell is formed of an 8 x 8 pixel array.

Each image cell **30b** has a single comparator reference line that services the entire cell. When a cell **30b** is being scanned, one of the parallel processors manages the reference voltage for that cell **30b** and records the digitized signals for all of the sensors in that cell. During the process of scanning the sensors in the cell

30b, the processor can simultaneously correlate the data from the cell to generate a preliminary estimate of the ridge flow direction in that cell. In the illustrated embodiment, a control processor 93 manages the sensor signal scanning and digitization, and supervises a bank of parallel processors 92 that perform feature extraction and matching functions. The other illustrated components are similar to those discussed above with reference to FIG. 11 and, hence.

Turning to FIG. 19, a 4 x 4 processor matrix circuit 180, such as might be used for a pipeline style implementation of the fingerprint minutiae processing, is illustrated. The circuit 180 includes an array of processors 184, a sensor array input/output portion 181, a non-volatile memory interface 182, and the illustrated multiprocessor array clock and control unit 182. The illustrated circuit 180 is used to identify and locate the fingerprint's unique minutiae to determine a match between a sensed fingerprint and one of a plurality of reference fingerprints. In other words, the processors 184 may match the minutiae against a set of previously stored reference minutia, to complete the identification process. When a positive identification has been made, for example, the circuit 180 may notify an external processor by sending an appropriately encrypted message over a host processor interface.

There is a general need to ensure sufficient contrast between the ridges and valleys of the fingerprint over the entire area of the fingerprint. The circuit 160 of FIG. 20 schematically illustrates a resistive network or matrix 161 including a plurality of interconnected resistors 162 for providing dynamic contrast enhancement for the array of pixels 30a. The effect of adjacent pixels is used to normalize the output of each pixel and while providing sufficient contrast. The circuit includes a pair of amplifiers 163, 164 for providing the enhanced contrast output signals.

Each pixel's value is determined by comparing the sensor signal to a reference signal that sums the block reference signal with a weighted average of the signals from all of the sensors in the immediate area. The square resistive grid or matrix provides the necessary weighted average to each of the pixel comparators simultaneously. The global block reference line 165 is preferably driven with a staircase waveform while the comparator outputs are monitored for change of state. Each pixel's gray-scale value may be determined by noting which step of the staircase causes that pixel's comparator to change state.

A variation for dynamic contrast enhancement is understood with reference to the circuit 170 of FIG. 21. Dynamic contrast enhancement can also be implemented by an array 172 of capacitors 171 interconnecting the pixel nodes 174. In this embodiment, the array 172 receives an alternating current signal derived from the synchronous demodulator 175 described in greater detail above. The capacitors 171 serve as an AC impedance network distributing and averaging the AC signals in a fashion analogous to the behavior of the resistive network 161 (FIG. 20) for DC signals. In the AC contrast enhancing circuit 170, the lowpass filtering that in other embodiments may be part of the demodulator circuit, is moved to the comparator 177 circuit portion. The capacitor array 172 is readily implemented using conventional semiconductor processing techniques and may offer an advantage of relatively small size as compared to the resistor array implementation.

The resistive matrix circuit 160 and capacitor matrix circuit 170 may provide weighting for image contrast enhancement. An alternative is to conduct such enhancement via downstream software which may take a relatively long time to fully process. Accordingly, the resistor matrix and capacitor matrix arrangement may provide greater overall processing speed. In addition, such preliminary processing at the sensor 30 may allow relaxation of A/D conversion from an 8 bit AD converter to a 1 bit converter in some embodiments, while still providing high speed and at a relatively low cost. For example, processing of the fingerprint image and determination of a match may desirably take only several seconds for certain applications to avoid user frustration.

Referring to FIG. 22, another aspect of the invention is described wherein the sensor 30 may be contained within a secure sensor package 190. The sensor 30 is desirably mounted to prevent flexing or shifting which may stress the chip or its electrical connections. More particularly, the overall package may include a tamper resistant housing 191. For example, the housing 191 may be formed of a hard plastic material or metal that is strong and resistant to cutting, abrading or sawing. Alternately, the housing 191 may be a material which crumbles and destroys its internal circuit components if cutting, dissolution, or other forms of entry are attempted.

The sensor package 190 also includes the illustrated substrate 195, processor 192, destructible memory 195, and encrypted output circuit 194. More particularly, the encrypted output circuit 194 provides an output signal that can only be decrypted by the intended downstream device. The specification of U.S. Patent Nos. 4,140,272; 5,337,357; 4,993,068 and 5,436,972 each disclose various approaches to encryption.

The output of the sensor package 190 may be communicated to associated downstream decryption equipment via electrically conductive leads or pins, or may be inductively or optically coupled to associated equipment as will be readily understood by those skilled in the art. As would also be understood by those skilled in the art, electrical or other types of protection may be provided on the encrypted output portion to ensure that data, such as a database of fingerprints stored on the memory 193, is not readily readable by external connections and/or signal manipulations.

The sensor 30 and processor 192 may be configured to provide any of a range of integral sensor processing features. For example, the encrypted output may be a raw image, a processed image, fingerprint

minutiae data, a yes/no match indication, or personal identification and digital signature keys.

The illustrated sensor package **190** also includes a bead **196** of sealing material at the interface between the upper dielectric layer **52** of the sensor **30** and the adjacent portions of the housing **191**. Other sealing arrangements are also contemplated by the present invention, for desirably providing a fluid tight seal at the interface between the exposed upper dielectric layer and the adjacent housing portions. In addition, a cleaning liquid may be used to routinely clean the window and reduce the contamination thereof. Since various alcohols, such as isopropyl alcohol are likely to be used as cleaning solutions, the housing **191** and sealing bead **196** are desirably resistant to such chemicals.

Turning to FIG. 23 another sensor package **220** is illustrated, and the problems and solutions with respect to an integrated circuit package in accordance with the present invention are discussed. As would be readily understood by those skilled in the art, a fingerprint sensor integrated circuit presents a special packaging difficulty since it has to be touched by the finger being scanned. It is typically desired to avoid touching of an integrated circuit in conventional integrated circuit fabrication, in part, because of potential contamination. The main contaminants of concern are sodium and the other alkaline metals. These contaminants may cause mobile ions in the SiO_2 layers that are typically used to passivate the integrated circuit. The resulting oxide charge degrades device characteristics especially in MOS technology.

One conventional approach to controlling mobile ionic contamination uses hermetic packaging with a phosphorus-doped passivation layer over the integrated circuit. The phosphorus doping reduces contaminant mobility by trapping mechanisms as would be readily understood by those skilled in the art. Plastic packaging has now become more widespread, and a silicon nitride passivation layer may be used with the plastic packaging. Silicon nitride may greatly reduce the permeability to contaminants to permit direct contact between the finger of the user and the integrated circuit. Accordingly, silicon nitride may preferably be used as a passivation layer of the fingerprint sensor in accordance with the present invention.

A fingerprint sensor as in the present invention also raises several unique packaging requirements including: the package needs to be open to enable finger-to-sensor die contact; the package should be physically strong in order to withstand rough use; the package and die should be able to withstand repeated cleaning with detergent and/or disinfectant solutions, and including scrubbing; the die should be able to withstand contact with a wide variety of organic and inorganic contaminants, and should be able to withstand abrasion; and finally the package should be relatively inexpensive.

The illustrated package **220** of FIG. 23 addresses these packaging issues. The package **220** includes an integrated circuit die **221** mounted on a metal paddle **222** that is connected to the leadframe **223** during injection molding of the surrounding plastic material **191** of the package. Connections are made by bond wires **227** and the lead frame **223** to the outwardly extending leads **228** as would be readily understood by those skilled in the art. The upper surface of the plastic housing **191** includes an integrally molded opening **52** which permits contact to the die **221**. The adhesion between the plastic molding compound and the adjacent upper surface portions of the die creates a seal in this illustrated embodiment.

The integrated circuit die **221** may also include a passivation layer **224** of silicon nitride for reasons highlighted above. In addition, as shown in the illustrated sensor package **220**, the die **221** may be provided with a second protective coating **225**. Each of the coatings **224, 225** are desirably relatively thin, such as on the order of about a micrometer, in order to retain sensor sensitivity. The outer coating **225** may be an organic material, such as polyimide or PTFE (Teflon™) which yields advantages in wear resistance and physical protection. Inorganic coatings, such as silicon carbide or amorphous diamond, may also be used for the outer layer **225** and may greatly enhance wear resistance, especially to abrasive particles. In addition, the material of the protective die coating **225** is preferably compatible with standard IC pattern definition methods in order to enable bond pad etching, for example.

The bond pads on the integrated circuit die **221** may be provided by aluminum. Another perhaps more preferable approach seals the pads with a gold plug, as may be applied by electroplating. In order to reduce the height created by the looped bond wires **227**, the die **221** may be directly flip-chip bonded in another embodiment of the invention, not shown. The sensor package **220** in other embodiments may be manufactured using tape automated bonding techniques.

Returning to FIG. 22, the sensor package **190** is that the memory **198** and/or other integrated circuit components may be made to destruct or be rendered secure upon breach of the housing **191**, for example. A coating **193** of material may be applied to the integrated circuit die(s) that causes destruction of the die if the coating is dissolved away. The memory **193** may also self-destruct or empty its contents upon exposure to light or upon removal of a sustaining electrical current. Those of skill in the art will readily appreciate other approaches to ensuring the integrity of the data and processing capabilities of the sensor package **190**. Accordingly, the present invention provides that sensitive data, such as a database of authorized fingerprints, encryption keys, or authorization codes, are not readily stolen from the sensor package **190**. In addition, although the sensor package **190** may desirably incorporate the electrical field sensor **30** as described extensively herein, other sensors are also contemplated for inclusion with a secure sensor package.

The various embodiments of the sensor **30** and its associated processing circuitry may implement any of a

number of conventional fingerprint matching algorithms.

Fingerprint minutiae, that is, the branches or bifurcations and end points of the fingerprint ridges, are often used to determine a match between a sample print and a reference print database. Such minutiae matching may be readily implemented by the processing circuitry. For example, in the specification of U.S. Patent Nos. 3,859,633 and 3,893,080 are directed to fingerprint identification based upon fingerprint minutiae matching. The specification of U.S. Patent No. 4,151,512 describes a fingerprint classification method using extracted ridge contour data. The specification of U.S. Patent No. 4,185,270 discloses a process for encoding and verification also based upon minutiae. The specification of U.S. Patent No. 5,040,224 discloses an approach to preprocessing fingerprints to correctly determine a position of the core of each fingerprint image for later matching by minutiae patterns.

Turning to FIGS. 24-26 another significant aspect of the present invention is described. Because of the relatively fast and efficient processing of a fingerprint image provided by above identified sensor **30** and associated circuitry of the invention, the user may be provided with nearly real-time feedback regarding positioning of his finger on a fingerprint sensor, such as the illustrated electric field sensor **30**. Accordingly, the user may quickly and accurately reposition his finger, have his identification accurately determined, and promptly move forward with the intended task. In the past only a simple go or no-go indication has been described for a user as in the specification of U.S. Patent No. 4,947,443 for example, and with such an indication most likely taking a relatively long time. It is generally understood that unless such an indication can be given within several seconds, user frustration is likely to rise dramatically with any further passage of time. Moreover, a simple go/no-go indication may only prompt the user to try again without any useful guidance on what may be causing the no-go indication.

The apparatus **200** (FIG. 24) illustratively includes a fingerprint sensor **30** operatively connected to an image processor **201**. Along the lines as discussed above, the image processor **201** may include the tapped delay line or other functional center point calculator **202** for determining a center point from the sensed fingerprint as will be readily appreciated by those skilled in the art. The location of the center point relative to a predetermined reference center point may be determined and an indication given the user via a position indicator **203**. The image may also be further analyzed, and if the applied finger pressure is too great or too little, such an indication may also be given to the user. Accordingly, potential user frustration may be significantly reduced. A need to clean the sensor may also be effectively communicated to the user if repositioning and/or pressure changes are ineffective, such as after a predetermined number of attempts.

Turning to FIG. 25, a practical implementation of the position feedback sensing and indication is further described as applied in a computer workstation, such as the illustrated notebook computer **35** of the type including a keyboard **36** and display **37**. The applicability of this aspect of the invention to many types of fixed and portable computer workstations in addition to the illustrated notebook computer.

The fingerprint sensor **30** receives the finger of the user. The processor of the computer in cooperation with the fingerprint sensor **30** generates a display of the fingerprint image **206** along with its center point **205** on an image of a window **207** on the display **37**. In the illustrated embodiment, the display also includes a target center point **208** to assist the user is repositioning his finger for an accurate reading.

In addition to the visual image indication, a further indication may be given by display of the words "move upward" and "move left" along with the illustrated associated directional arrows. An indication may also be given concerning a desired pressure, such as the illustrated words "increase pressure".

Yet another variation of the feedback and pressure indications may be in the form of synthetically generated speech messages issued from a speaker **39** mounted within the housing of the computer. For example, the generated voice messages illustratively include an annunciation to "move finger up and to the left" and "increase finger pressure". Other helpful messages are also contemplated by the present invention.

Still another embodiment of finger position feedback sensing and indication is understood with further reference to the apparatus **210** of FIG. 26. In this embodiment, the sensor **30** is used to operate an access controller **211** which, in turn, may operate a door, for example, to permit a properly identified user to enter. Simple visual indications in the form of LEDs **212**, **213** for up and down motion, and left and right motion, respectively, may be provided to indicate to the user the proper positioning or repositioning of his finger. The illustrated embodiment also includes a plurality of LEDs **214** for indication of pressure.

A fingerprint sensor package includes a tamper-resistant housing, a fingerprint sensor mounted in the housing, an encryption output circuit mounted within the housing and operatively connected to the fingerprint sensor for generating an encrypted output signal related to a sensed fingerprint. The fingerprint sensor package may include a processor operatively connected between the fingerprint sensor and the encryption circuit. The package includes a reference fingerprint memory for storing reference fingerprint information. The processor has the capability to determine if a sensed fingerprint matches a stored reference fingerprint. A removing circuit is provided for removing reference fingerprint information from the reference fingerprint storage means responsive to tampering.

Claims

1. A fingerprint sensor package comprising:

   a tamper-resistant housing; a fingerprint sensor mounted in said housing; and encrypting output means mounted within said housing and operatively connected to said fingerprint sensor for generating an encrypted output signal related to a sensed fingerprint, with a processor operatively connected between said fingerprint sensor and said encrypting output means.

2. A fingerprint package as claimed in Claim 2 wherein reference fingerprint storage means for storing reference fingerprint information, and said processor comprises reference fingerprint matching means for determining if a sensed fingerprint matches a stored reference fingerprint.

3. A fingerprint package as claimed in Claim 3 wherein removing means for removing reference fingerprint information from said reference fingerprint storage means responsive to tampering.

4. A fingerprint package as claimed in any one of claims 1 to 3 wherein said fingerprint sensor comprises an integrated circuit having an outer surface portion for receiving a finger adjacent thereto, and said housing includes an opening therethrough in registry with the outer surface portion of the integrated circuit.

5. A fingerprint package as claimed in Claim 4 wherein sealing means for sealing an interface between the outer surface portion of the integrated circuit and adjacent housing portions, preferably in which said sealing means comprises a bead of sealing material.

6. A fingerprint package as claimed in Claim 5 wherein said housing comprises a plastic material, and the sealing means comprises a hermetic seal between the plastic material and adjacent portions of the integrated circuit.

7. A fingerprint package as claimed in Claim 3 wherein said integrated circuit comprises an outermost silicon nitride layer, in which said integrated circuit comprises an outermost layer including one of silicon carbide and diamond, and said fingerprint sensor comprises an electric field fingerprint sensor, and preferably said electric field fingerprint sensor comprises:

   an array of electric field sensing electrodes;
   a dielectric layer adjacent said electric field sensing electrodes, said dielectric layer for receiving a finger adjacent thereto; and
   drive means for applying an electric field drive signal to said electric field sensing electrodes and adjacent portions of the finger so that said electric field sensing electrodes produce a fingerprint image signal with a finger electrode exposed on an outer surface of said housing.

8. A fingerprint sensor package comprising:

   a tamper-resistant housing;
   a fingerprint sensor mounted in said housing;
   reference fingerprint storage means positioned within said g for storing reference fingerprint information;
   a processor operatively connected to said fingerprint sensor and said reference fingerprint storage means for determining if a sensed fingerprint matches a stored reference fingerprint, and removing means for removing reference fingerprint information from said reference fingerprint storage means responsive to tampering.

9. A fingerprint package as claimed in any one of Claims 1 to 7 or 8 including encrypting output means mounted within said housing and operatively connected to said processor for generating an encrypted output signal related to a sensed fingerprint, and said fingerprint sensor comprising an integrated circuit having an outer surface portion for receiving a finger adjacent thereto, and said housing including an opening therethrough in registry with the outer surface portion of the integrated circuit.

10. A fingerprint sensor package comprising:

   a housing having an opening therethrough;
   a fingerprint sensor mounted in said housing and comprising an integrated circuit having an outer surface portion for receiving a finger adjacent thereto and with said integrated circuit being positioned so that the outer surface portion is aligned in registry with the opening of said housing; and
   sealing means positioned to seal an interface between the outer surface portion of the integrated circuit and adjacent housing portions, in which said sealing means comprises a bead of sealing material, with said housing comprising a plastic material, and sealing means comprises a hermetic seal between the plastic material and adjacent portions of the integrated circuit, including encrypting output means mounted within said housing and operatively connected to said fingerprint sensor for generating an encrypted output signal related to a sensed fingerprint, and a processor operatively connected to said fingerprint sensor.

11. A method for making and securely operating a fingerprint sensor package of a type including a fingerprint sensor, the method comprising the steps of:

mounting the fingerprint sensor within a tamper-resistant housing;
generating within the tamper-resistant housing an encrypted output signal related to a sensed fingerprint from the fingerprint sensor, storing reference fingerprint information within the housing and
determining within the tamper-resistant housing if a sensed fingerprint matches a stored reference fingerprint.

12. A method as claimed in Claim 11 including the steps of removing reference fingerprint information from within the tamper-resistant housing responsive to tampering, forming an integrated circuit fingerprint sensor having an outer surface for receiving a finger adjacent thereto;

mounting the integrated circuit fingerprint sensor within a housing having an opening therethrough so that the opening is in registry with the outer surface portion of the integrated circuit; and
sealing an interface between the outer surface portion of the integrated circuit and adjacent housing portions, with the step of mounting comprising molding a plastic material surrounding the integrated circuit, and the step of sealing comprises hermetically sealing an interface between the plastic material and adjacent portions of the integrated circuit.

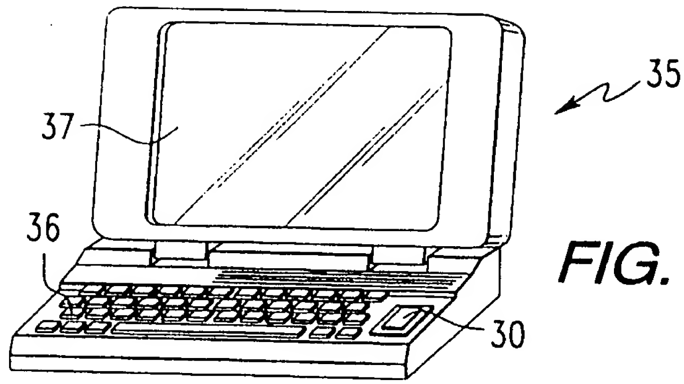


FIG. 1

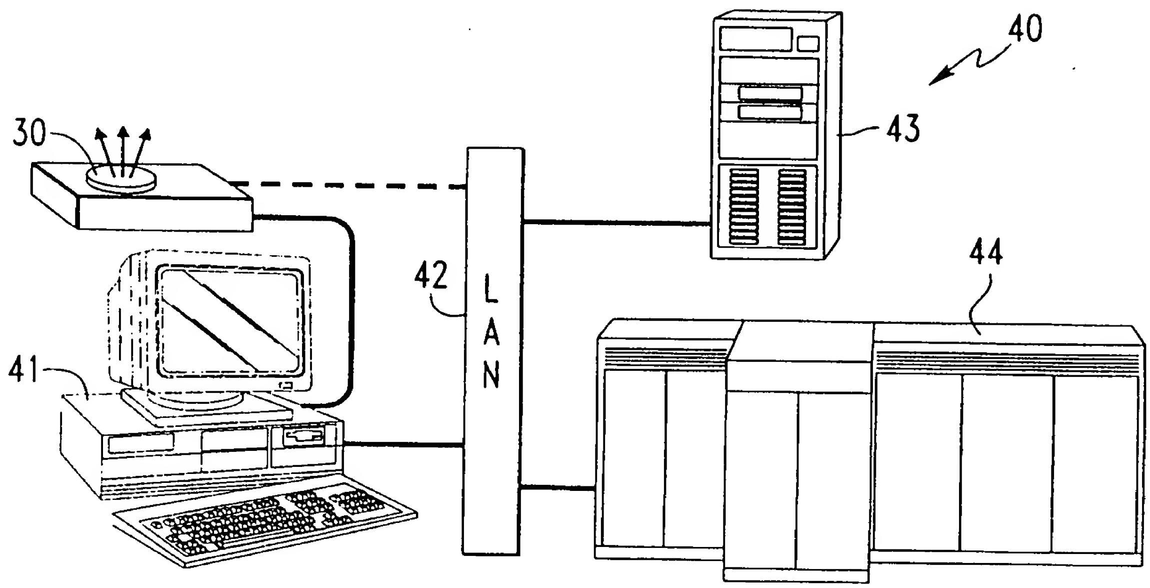


FIG. 2

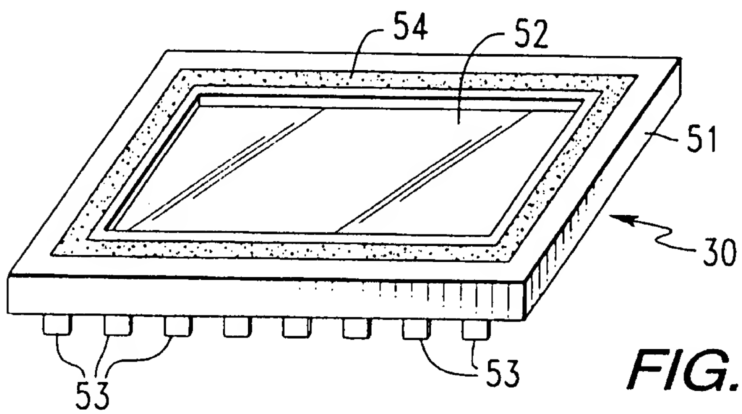


FIG. 3

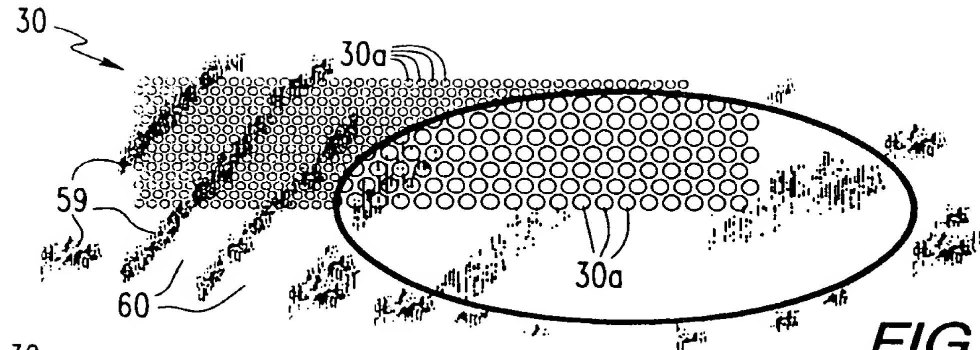


FIG. 4

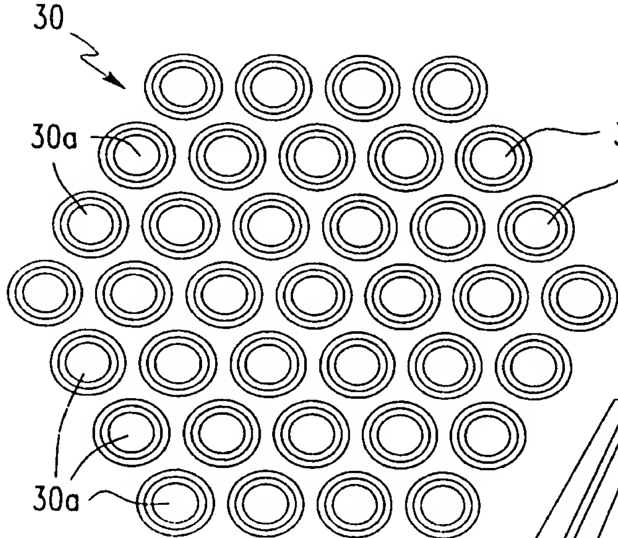


FIG. 5

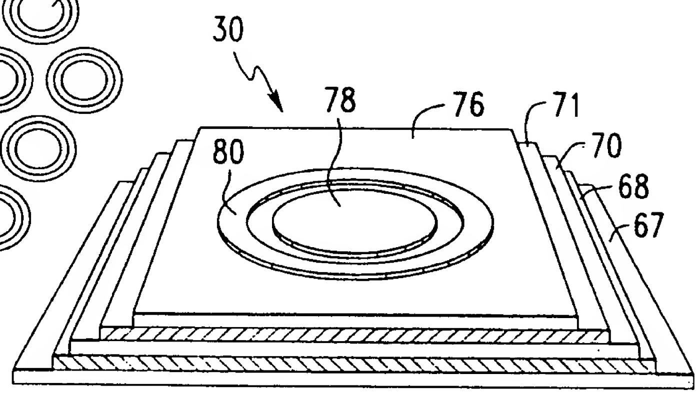


FIG. 6

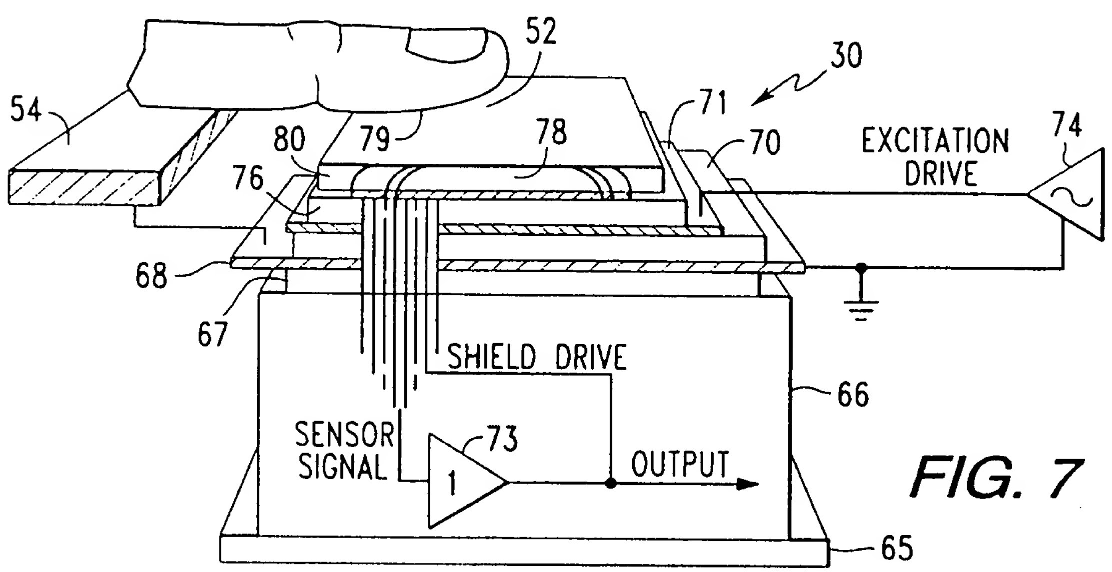


FIG. 7

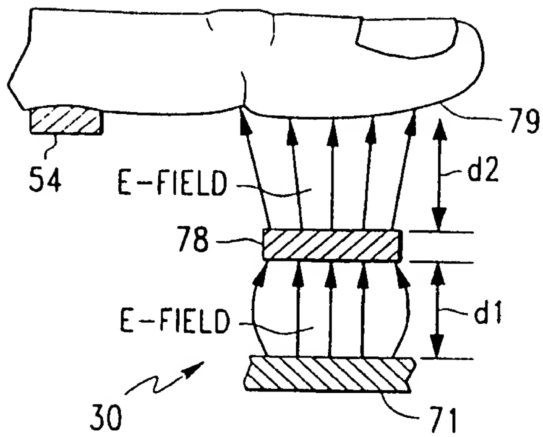


FIG. 8

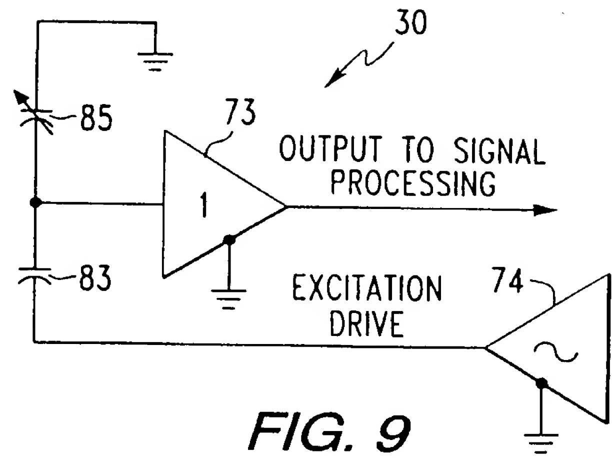


FIG. 9

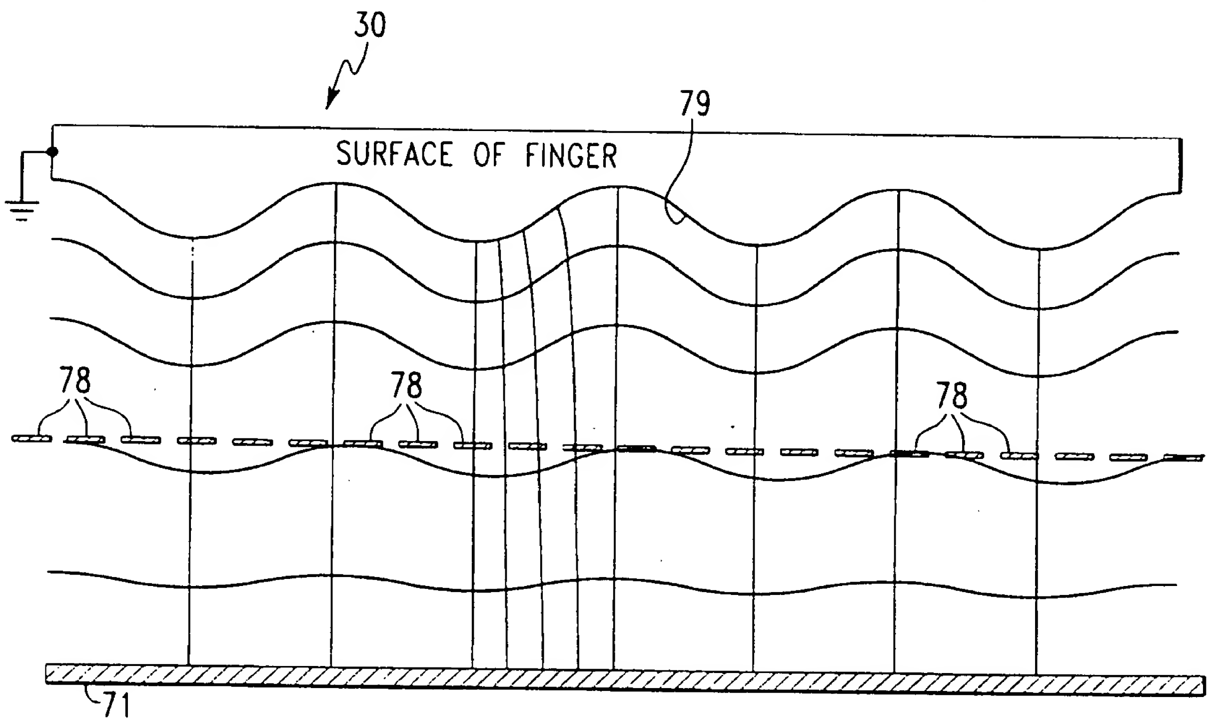


FIG. 10

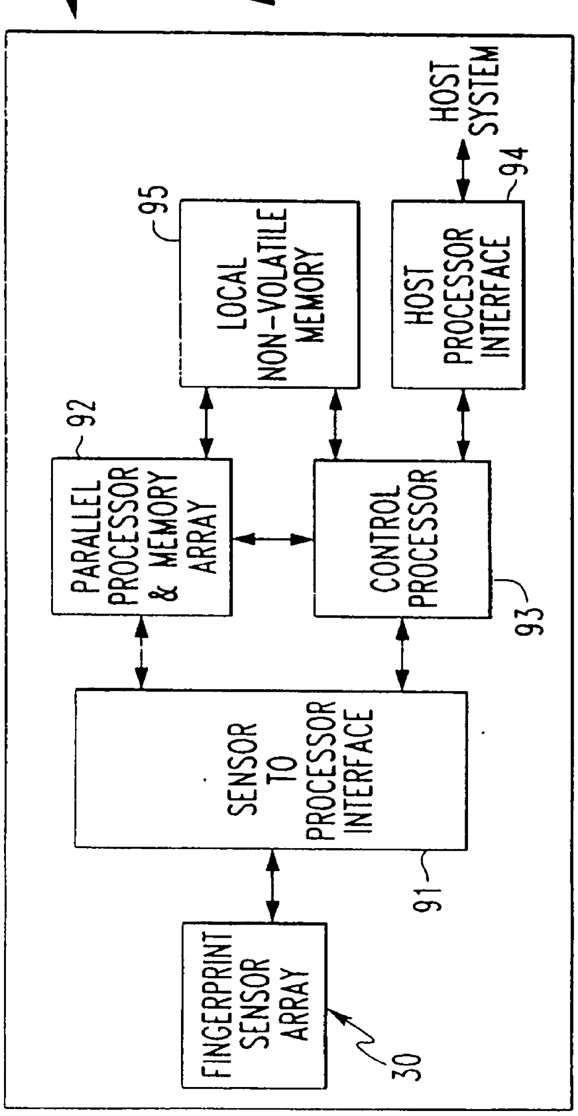
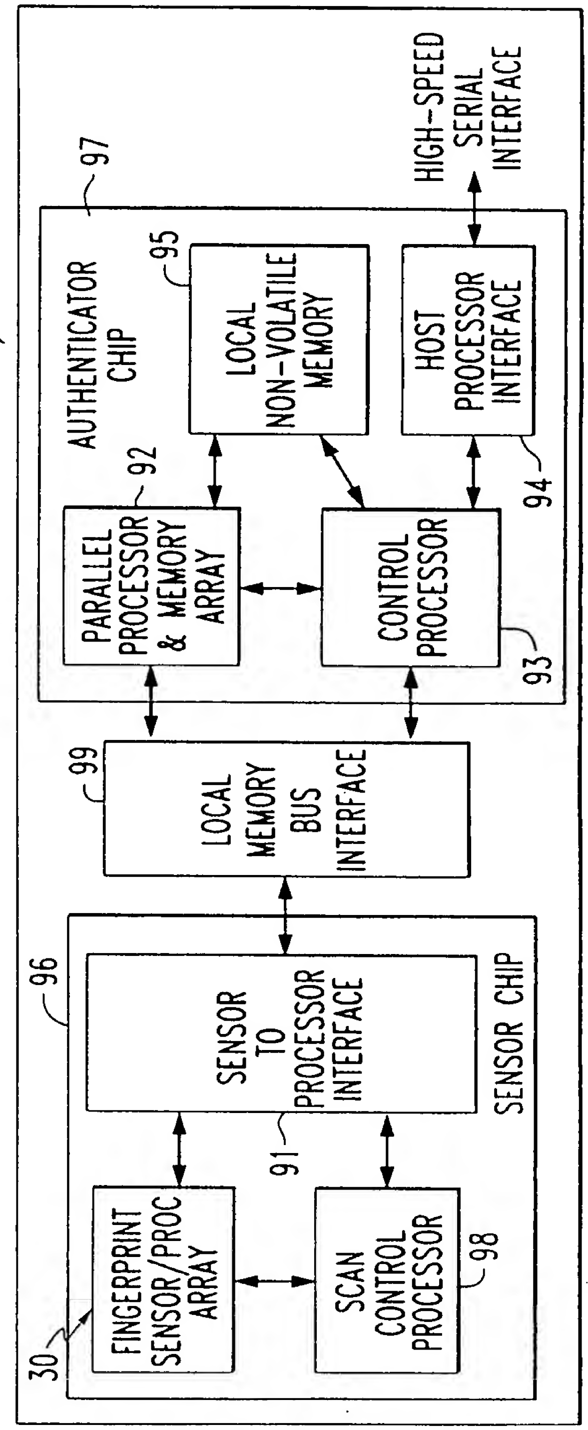


FIG. 11



100

FIG. 12

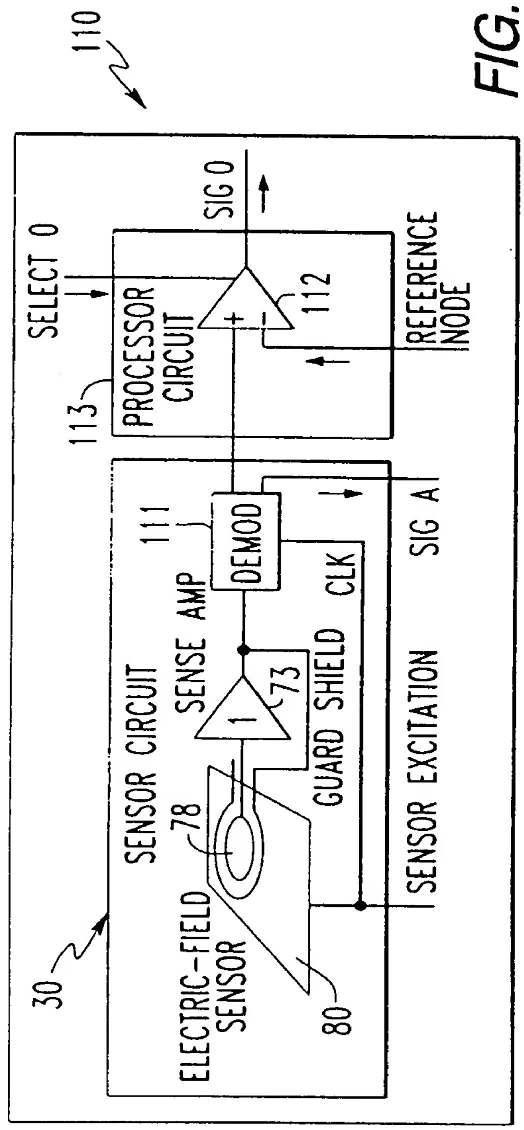

110
SELECT 0
PROCESSOR CIRCUIT
113
112
SIG 0
REFERENCE NODE
SENSOR CIRCUIT
SENSE AMP
111
DEMOD
73
78
ELECTRIC-FIELD SENSOR
30
80
GUARD SHIELD
CLK
SIG A
SENSOR EXCITATION

FIG. 13

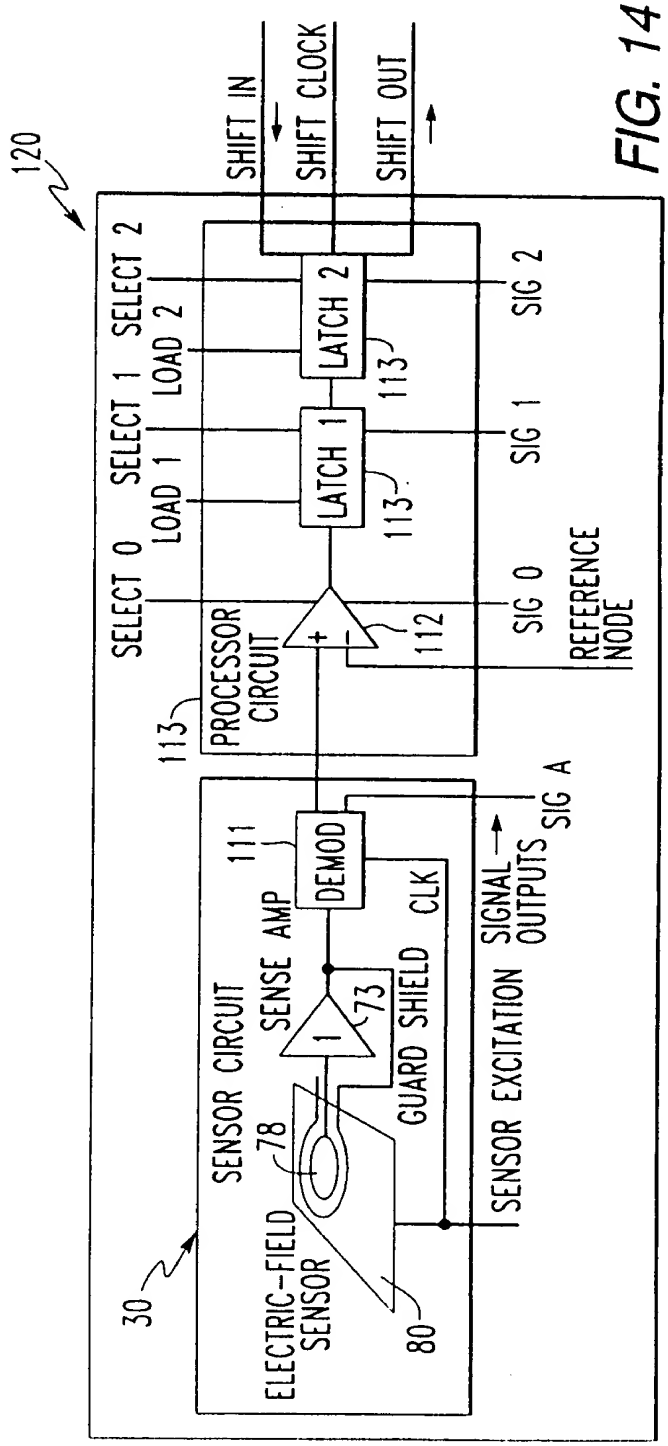
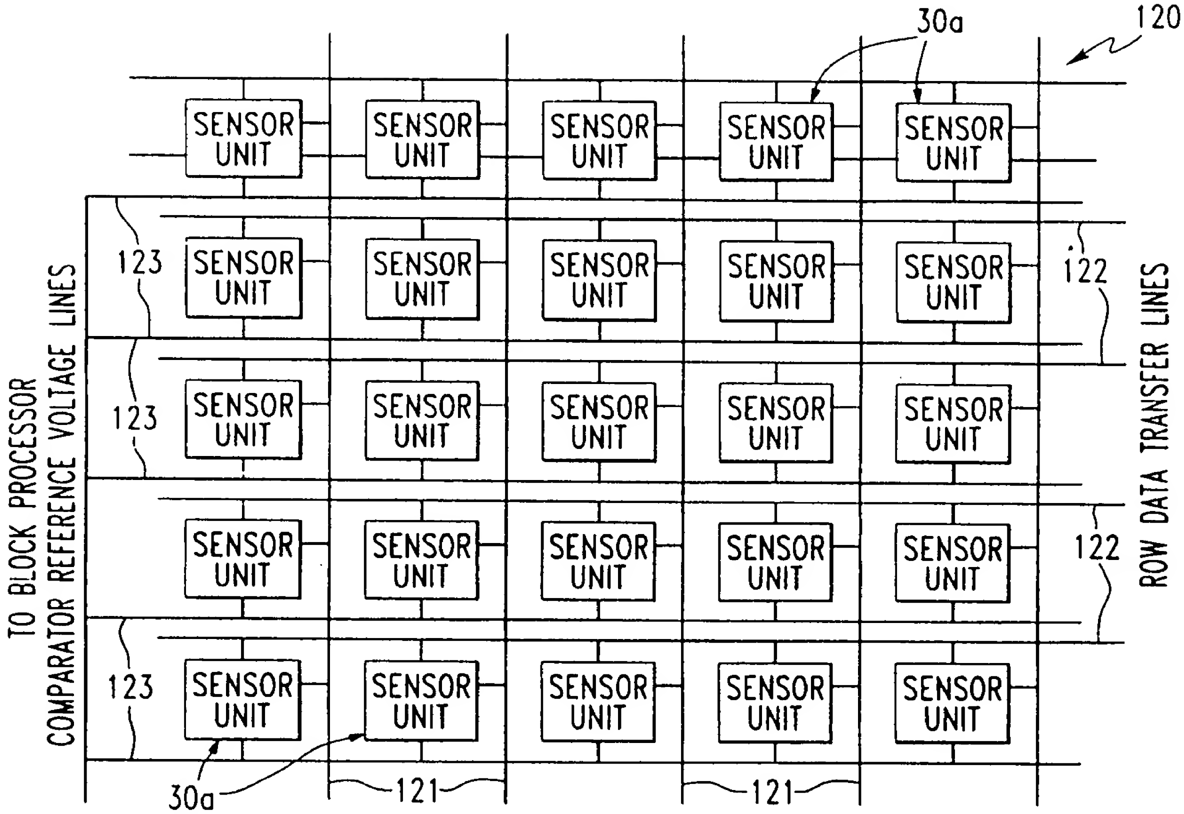
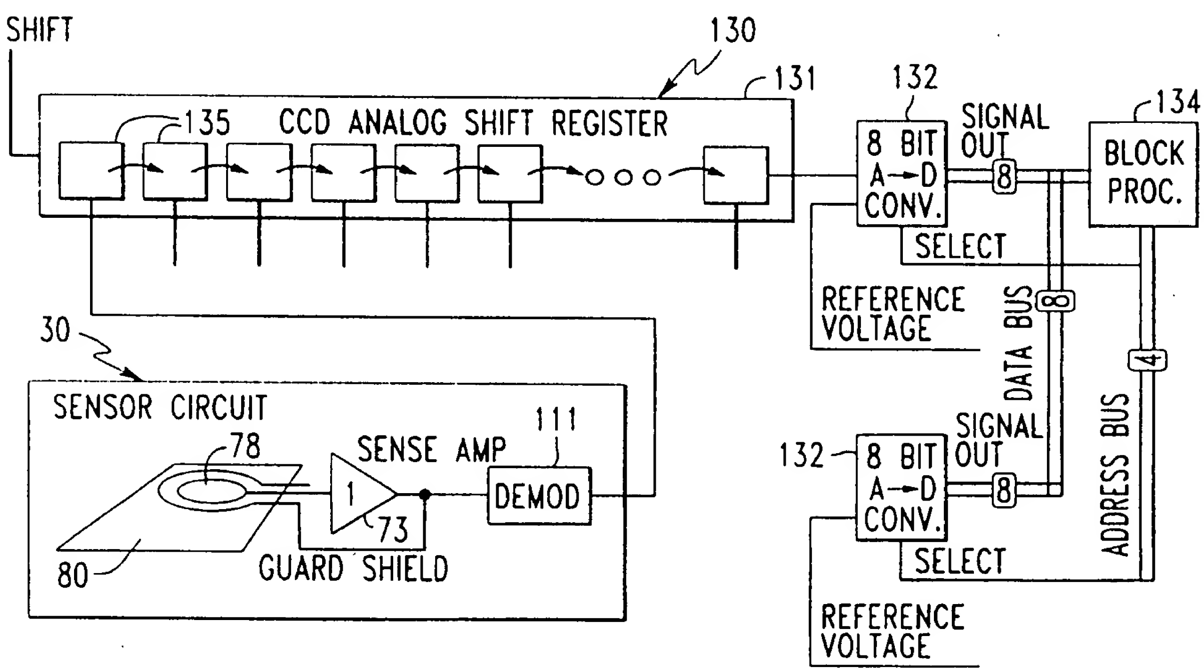

120
SHIFT IN
SHIFT CLOCK
SHIFT OUT
SELECT 0
LOAD 1
SELECT 1
LOAD 2
SELECT 2
LATCH 1
LATCH 2
113
SIG 0
SIG 1
SIG 2
REFERENCE NODE
PROCESSOR CIRCUIT
112
SENSOR CIRCUIT
SENSE AMP
111
DEMOD
SIG A
SIGNAL OUTPUTS
CLK
73
78
GUARD SHIELD
ELECTRIC-FIELD SENSOR
30
80
SENSOR EXCITATION

FIG. 14



30a
120
SENSOR UNIT
123
122
TO BLOCK PROCESSOR
COMPARATOR REFERENCE VOLTAGE LINES
ROW DATA TRANSFER LINES
30a
121
COLUMN DATA TRANSFER LINES

FIG. 15



SHIFT
130
131
132
135
CCD ANALOG SHIFT REGISTER
8 BIT A→D CONV.
SIGNAL OUT
8
BLOCK PROC.
134
SELECT
REFERENCE VOLTAGE
DATA BUS
4
ADDRESS BUS
30
SENSOR CIRCUIT
78
SENSE AMP
111
1
DEMOD
73
80
GUARD SHIELD

FIG. 16

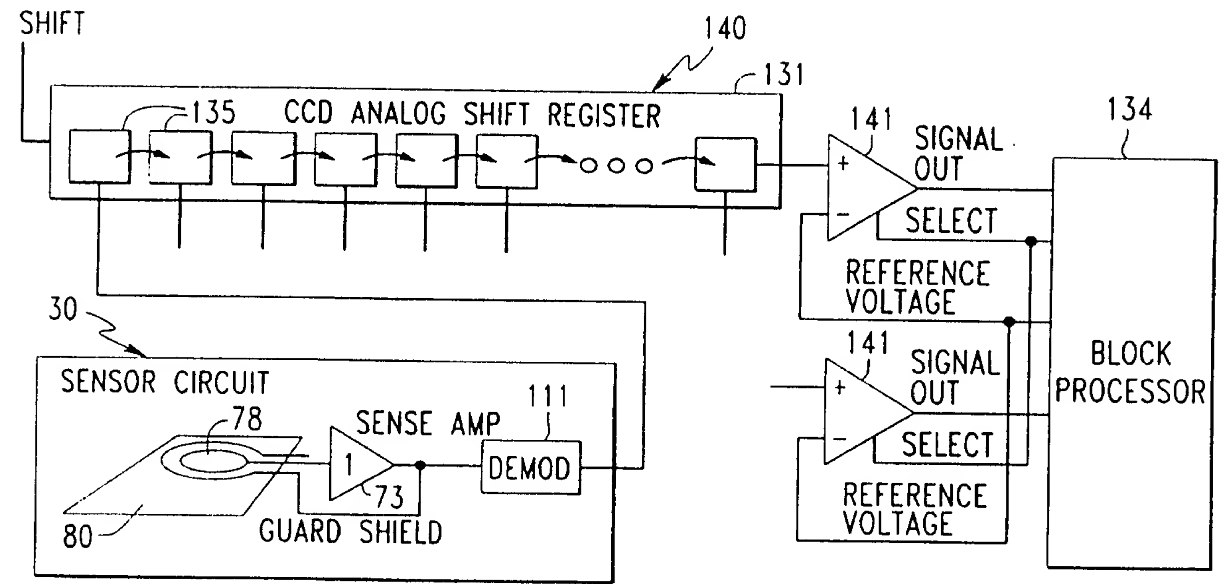

SHIFT
140
131
135
CCD ANALOG SHIFT REGISTER
141
SIGNAL OUT
134
SELECT
REFERENCE VOLTAGE
30
141
SIGNAL OUT
BLOCK PROCESSOR
SENSOR CIRCUIT
111
78
SENSE AMP
1
DEMOD
SELECT
73
REFERENCE VOLTAGE
80
GUARD SHIELD

FIG. 17

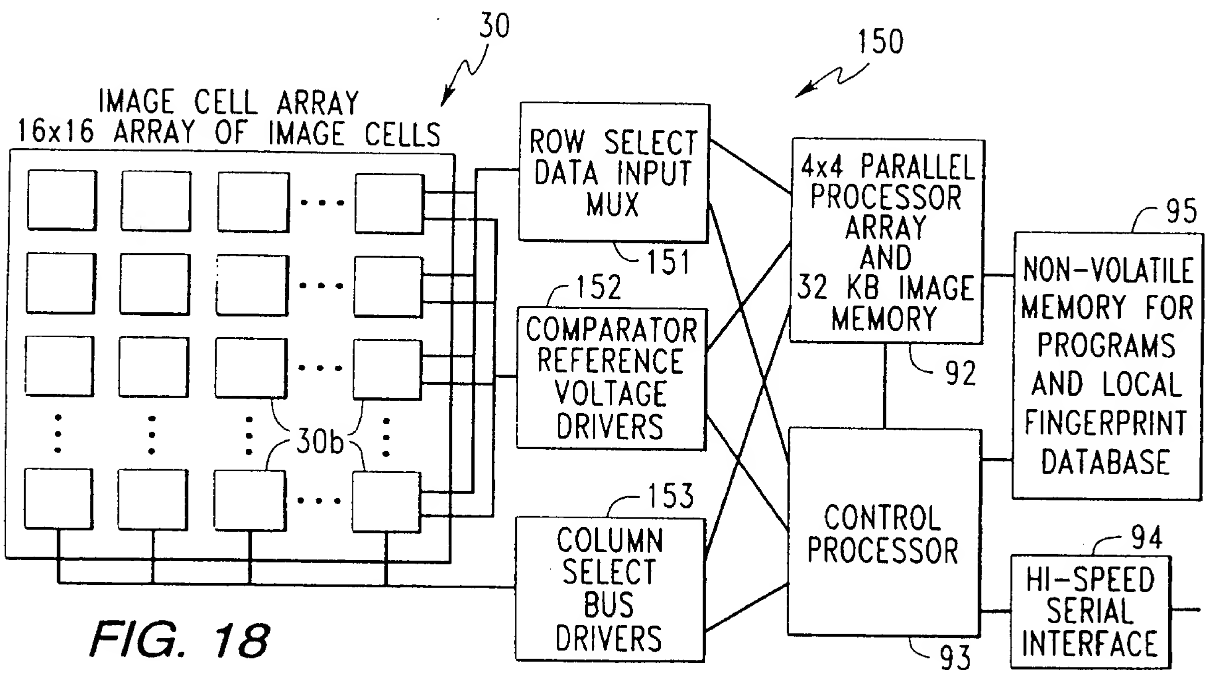

30
150
IMAGE CELL ARRAY
16x16 ARRAY OF IMAGE CELLS
ROW SELECT DATA INPUT MUX
4x4 PARALLEL PROCESSOR ARRAY AND 32 KB IMAGE MEMORY
95
151
152
NON-VOLATILE MEMORY FOR PROGRAMS AND LOCAL FINGERPRINT DATABASE
COMPARATOR REFERENCE VOLTAGE DRIVERS
92
30b
153
CONTROL PROCESSOR
94
COLUMN SELECT BUS DRIVERS
HI-SPEED SERIAL INTERFACE
93

FIG. 18

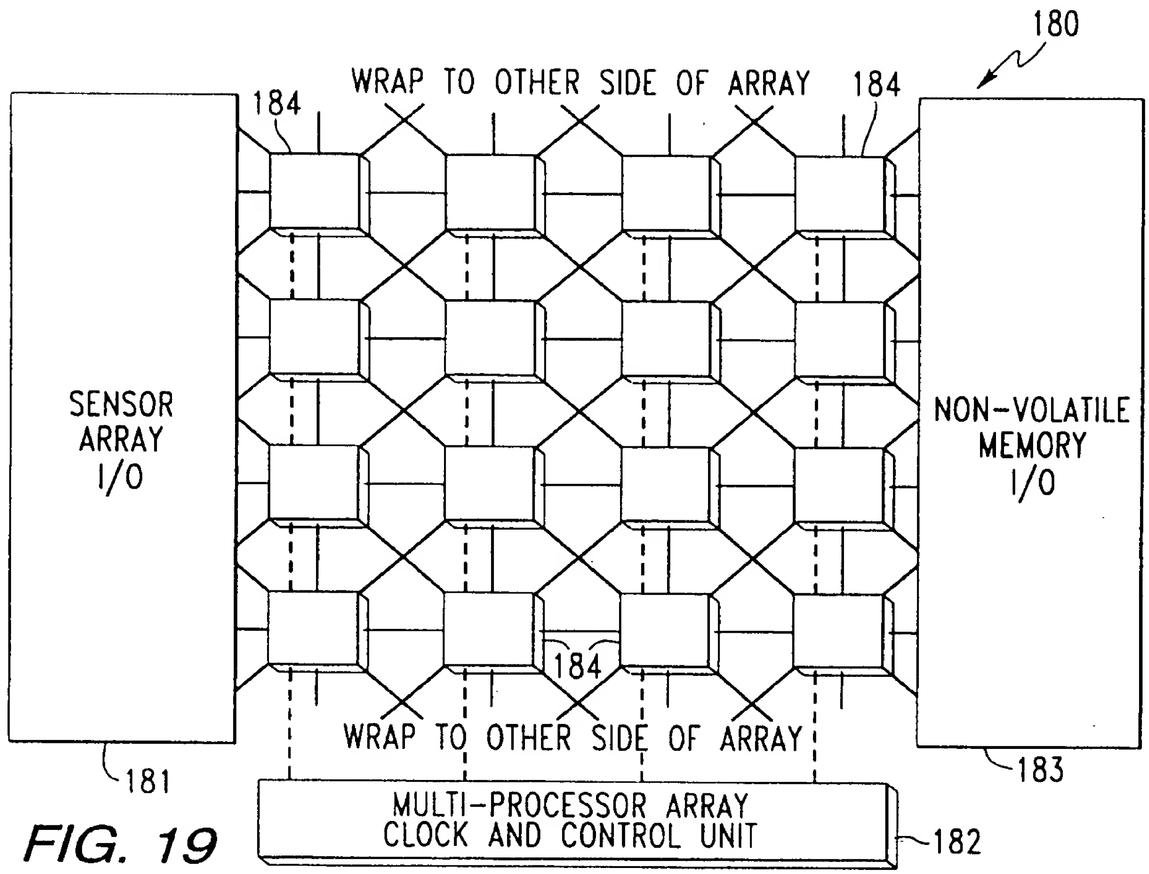

180
WRAP TO OTHER SIDE OF ARRAY
184
184
SENSOR ARRAY I/O
NON-VOLATILE MEMORY I/O
184
WRAP TO OTHER SIDE OF ARRAY
181
183
MULTI-PROCESSOR ARRAY CLOCK AND CONTROL UNIT
182

FIG. 19

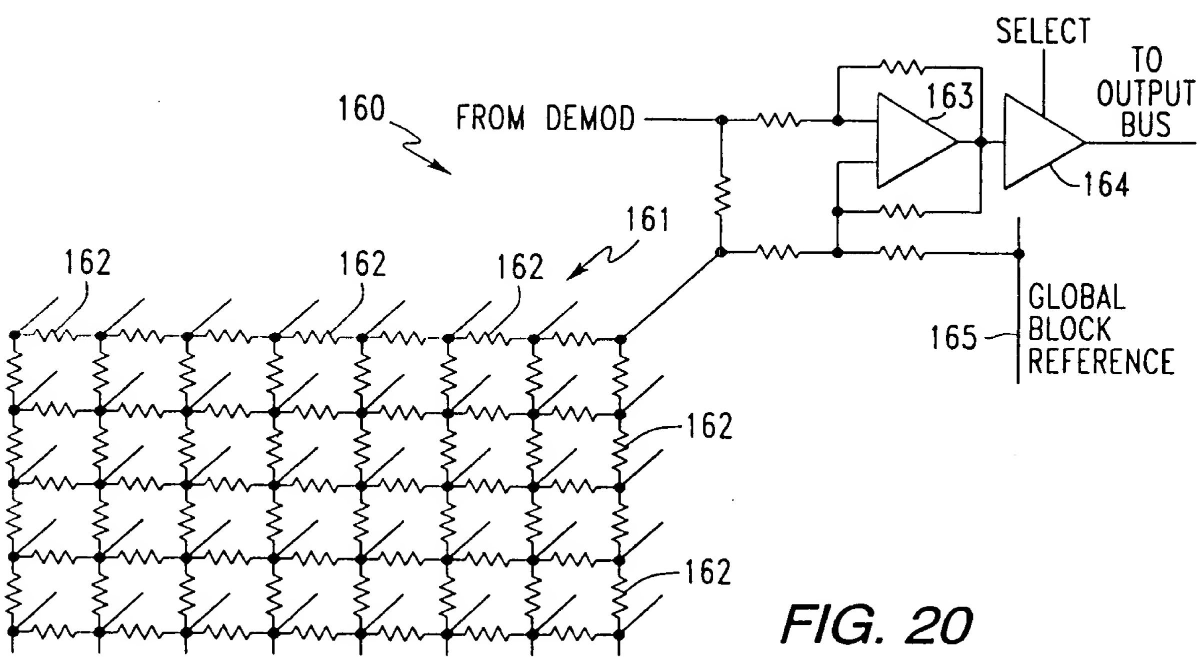

SELECT
TO OUTPUT BUS
160
FROM DEMOD
163
164
161
162
162
162
165
GLOBAL BLOCK REFERENCE
162
162

FIG. 20

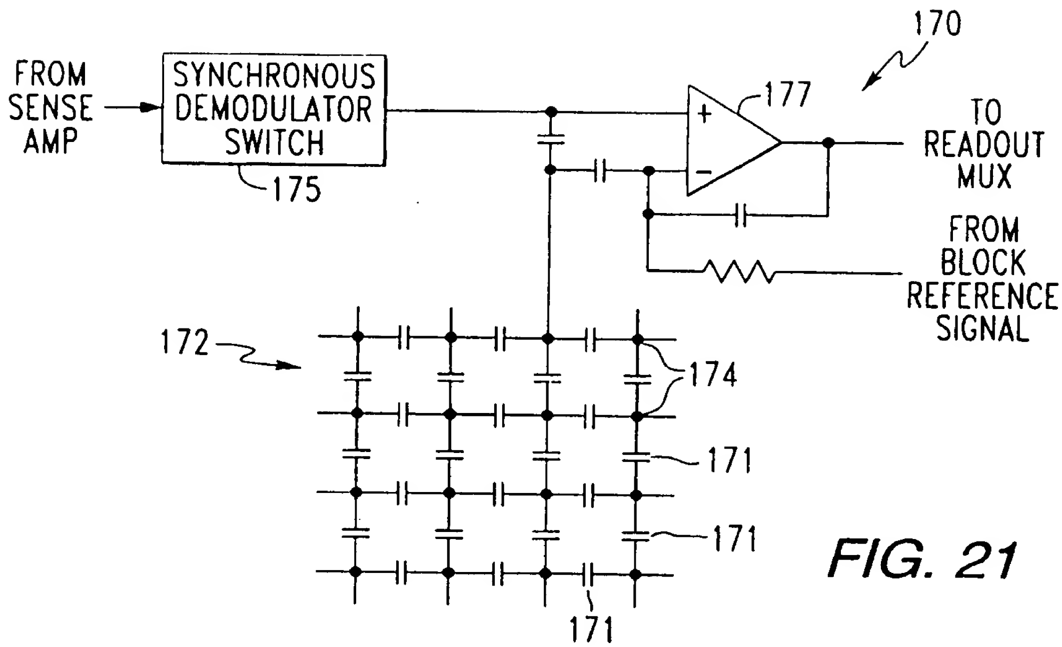


FIG. 21

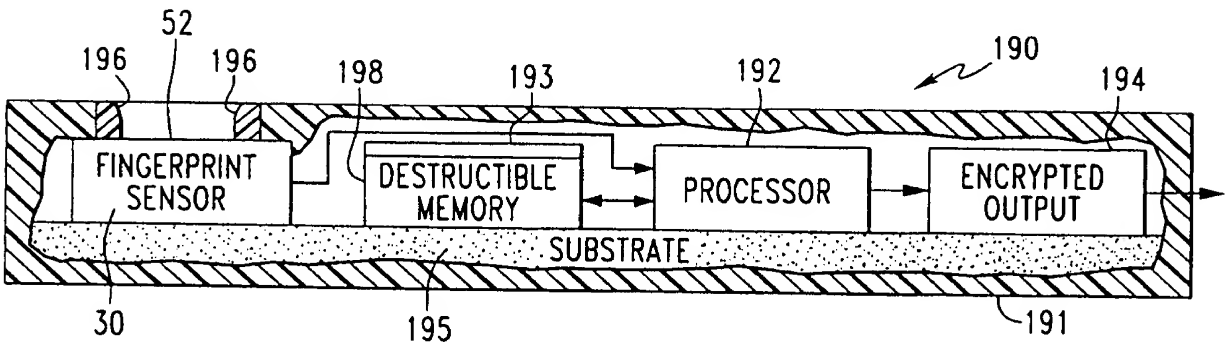


FIG. 22

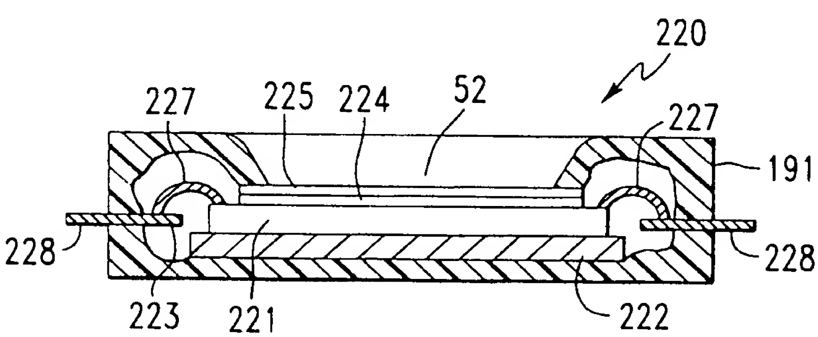


FIG. 23

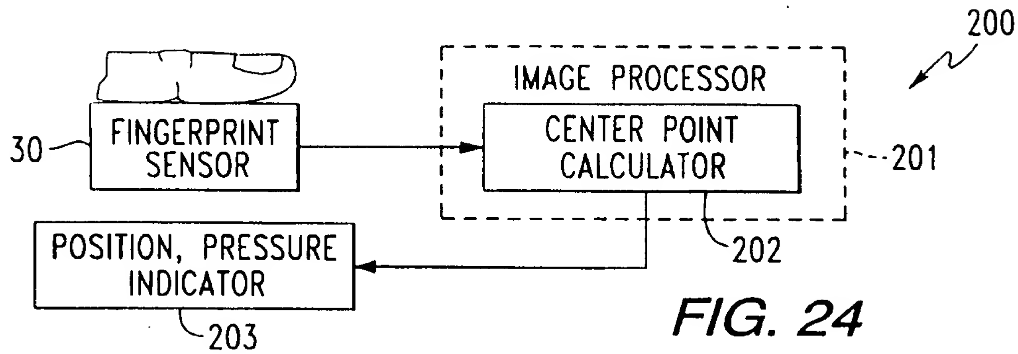


FIG. 24

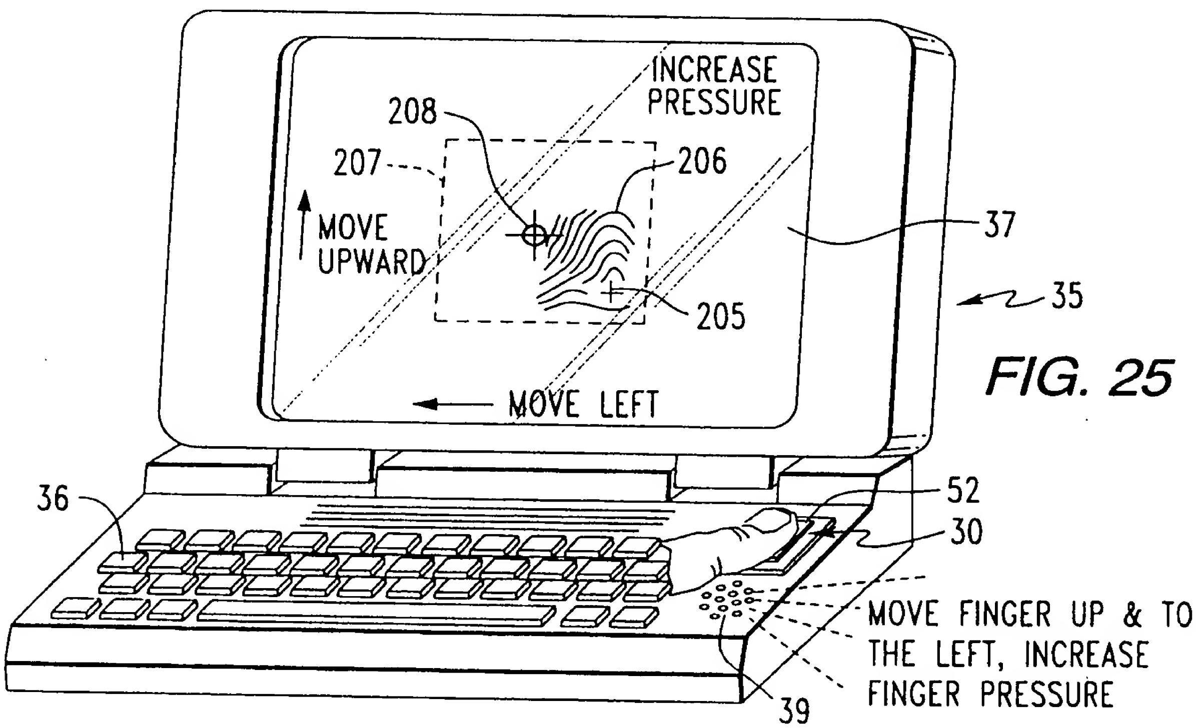


FIG. 25

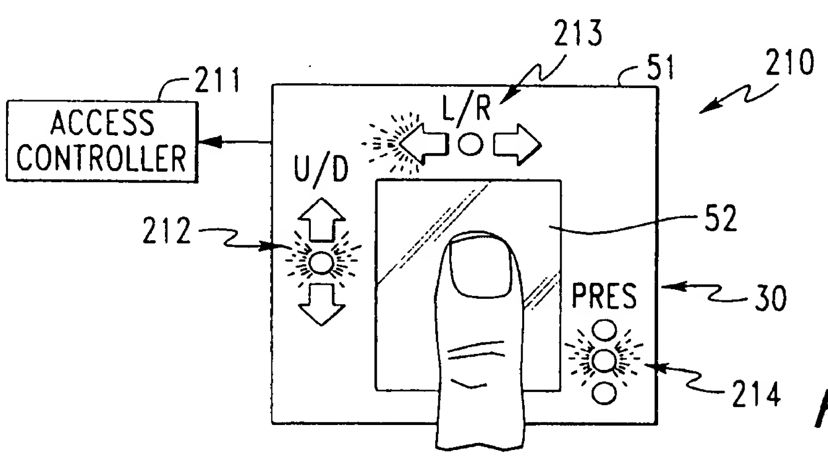


FIG. 26